UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/604,518	06/27/2000	John L. Manferdelli	MSFT-0187/154573.1	4937

7590 07/23/2004

Peter M Ullman
Woodcock Washburn Kurtz Mackiewicz & Norris LLP
One Liberty Place
46th Floor
Philadelphia, PA 19103

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2131	11

DATE MAILED: 07/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/604,518	MANFERDELLI ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28,30,31 and 33-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28,30,31 and 33-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detailed Office Action

Claims 1-28, 30-31, and 33-41 have been fully reconsidered and are pending.

Response to Arguments

Applicant's arguments with respect to claims 1,9, 20, 25, and 31 have been considered but are moot in view of the new ground(s) of rejection. On page 11 of the immediate action, Applicant has noted 3 features that have been amended into claim 1 and at least one of those features in claims 9, 20, 25, and 31. Applicant has made it clear on the record that at least one of these features has been added to the independent claims. Examiner would like to note a discrepancy found with the amendments in some of the claims and how they are discussed on page 11. Specifically feature (1) listed on page 11 proclaims that a key is stored in memory that is not accessible to the cryptographic algorithm. To the contrary, the amendment in claim 1 proclaims that a cryptographic key is stored in memory that is not accessible to said first of said plurality of secure repositories. Examiner has searched for the claimed amendment. Examiner would like to point out that there is a difference in not being accessible to the cryptographic algorithm and not being accessible to the secure repository.

Following this analysis, the Examiner would also note that claim 9 has neither of the above-mentioned features. Claim 9 proclaims that a key is applied but is not stored

in a memory. Because of the amendment intentions found on page 11 of the immediate action, the Examiner is interpreting claims 9, 20, and 25 to mean that the key is not stored in memory accessible to the software repositories. This interpretation is consistent with the language claimed in claims 1 and 31.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-28, 30-31, and 33-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies et al (USP 5,689,565) in view of Cassagnol et al (USP 6,385,727).

As per claim 1, Spies et al teach:

providing an interface, said interface being callable by said software process (column 3, line 17);

if said one of said plurality of secure repositories is said first of said plurality of secure repositories, providing a first set of computer-executable instructions which are invocable by said callable interface (column 17, line 14); and

if said one of said plurality of secure repositories is said second of said plurality of secure repositories, providing a second set of computer-executable instructions which are invocable by said callable interface, said second set of computer executable instructions being different from said first set of computer-executable instructions (figure 11, element 174).

Spies et al are silent in expressly disclosing that the first secure repositories comprises a software module that uses a cryptographic algorithm to apply a cryptographic key to data without said cryptographic key being stored in a memory accessible to said first secure repositories. Spies et al teach the use of cryptographic keys applied to data. Cassagnol teaches the idea of having memory in a highly protected environment whereby no other system components have accessed the isolated memory circuit (column 17, lines 1-15). Protecting memory, which stores secret keys, is advantageous to the security of the system. Blocking access to the memory by other components of the system, greatly improves the overall security of the system. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Cassagnol et al within the system of Spies et al because it would further isolate the secret keys to prevent key divulgence.

Spies et al are silent in expressly disclosing secure repositories comprises a hardware module that uses said cryptographic algorithm to apply said cryptographic key to data, said hardware module further comprising hardware that resists or prevents divulgence of said cryptographic key outside of said hardware module. Cassagnol

isolated memory circuit provides this function of tamper resistance (column 4, line 62—column 5, line 2). Tamper resistance is used to protect memory so that it cannot be accessed by external sources of any kind. This is advantageous to the security of the keys stored in the memory. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Cassagnol et al within the system of Spies et al because it would further increase the protection the cryptographic keys by placing tamper resistant hardware around them.

As per claim 2, Spies et al teach secure repository converts encrypted data to decrypted data using a cryptographic algorithm to apply a cryptographic key to said encrypted data, and wherein said software process performs an operation on said decrypted data (column 3, lines 25-30).

As per claim 3, Spies et al teach operation comprises rendering said decrypted data (column 3, line 27).

As per claim 4, Spies et al teach said first or said second sets of computer-executable instructions is provided in the form of an executable file dynamically linkable with said software process (column 3, line 30).

As per claim 5, Spies et al teach said interface comprises a first function callable by said software process, said first function being parameterized by first data representative of a type of secure repository (column 3, lines 10-20).

As per claim 6, Spies et al teach said interface is callable by said software process without regard to whether said one of said plurality of secure repositories is said first of said plurality of secure repositories or said second of said plurality of secure repositories (column 17, lines 1-8).

As per claim 7, Spies et al teach said interface comprises a second function callable by said software process, said second function requesting that said secure repository perform at least one action (column 17, lines 39-43).

As per claim 8, Spies et al teach first of said plurality of secure repositories executes on a closed-platform device, and wherein said second of said plurality of secure repositories executes on an open-platform device (column 18, lines 10-15).

As per claim 9, Spies et al teach a software process issuing a first interface call which authenticates said software process to said one of said plurality of secure repositories (column 17, lines 13-14); and

said software process issuing a second interface call which requests performance of an action by said secure repository for said software process (column 17, lines 40-45);

wherein said software process issues said first and second interface calls without regard to whether said one of said plurality of secure repositories is a first of said plurality of secure repositories or a second of said plurality of secure repositories (column 17, lines 1-8).

Examiner supplies the same rationale for the motivation as recited in the rejection of claim 1 to incorporate the teachings of Cassagnol et al within the system Spies et al.

As per claim 10, Spies et al teach secure repository converts encrypted data to decrypted data using a cryptographic algorithm to apply a cryptographic key to said encrypted data, and wherein said software process performs an operation on said decrypted data (column 3, lines 25-30).

As per claim 11, Spies et al teach operation comprises rendering said decrypted data (column 3, line 27).

As per claim 12, Spies et al teach first secure repository comprises a software-based secure repository, and wherein said second secure repository

comprises at least some isolated hardware (column 17, line 35, column 18, lines 12-13, and column 19, line 9).

Examiner supplies the same rationale for the motivation as recited in the rejection of claim 1 to incorporate the teachings of Cassagnol et al within the system Spies et al.

As per claim 13, Spies et al teach each of said first and second secure repositories are software-based repositories, said first secure repository having at least one feature not present in said second secure repository (column 17, line 33 and column 18, lines 10-20).

As per claim 14, Spies et al teach one of said plurality of secure repositories is said first of said plurality of secure repositories, and wherein said software process issues said first and second interface calls without regard to whether said second repository exists (column 17, lines 1-8).

As per claim 15, Spies et al teach first interface call is parameterized by first data representing a first type of secure repository, and wherein said first and said second of said plurality of secure repositories are each of said first type (column 17, lines 18-19, line 45).

As per claim 16, Spies et al teach software process performs a second action if said one of said plurality of repositories is either said first or said second of said plurality of secure repositories (column 17, line 14), and wherein said software process does not perform said second action if said one of said plurality of secure repositories is a third of said plurality of secure repositories, said third of said plurality of secure repositories being of a second type different from said first type (column 19, lines 45-65).

As per claim 17, Spies et al teach dynamically, linking to said software process a first set of computer-executable instructions, if said one of said plurality of repositories is said first of said plurality of secure repositories (column 18, lines 64-67); and

dynamically linking to said, software process a second set of computer-executable instructions different from said first set of computer-executable instructions, if said one of said plurality of secure repositories is said second of said plurality of secure repositories (column 19, lines 1-4).

As per claim 18, Spies et al teach the act of said software process receiving second data in response to said second interface call, said second data being generated by said one of said plurality of secure repositories, wherein said second data does not expose to said software process whether said data was generated by said first secure repository or said second secure repository (column 19, lines 30-44).

As per claim 19, Spies et al teach a computer-readable medium encoded with computer-executable instructions to perform the method of claim 9 (column 17, lines 33).

As per claim 20, Spies et al teach a first set of computer-executable instructions which converts encrypted data into decrypted data by applying a cryptographic key to said encrypted data (column 3, lines 25-30); and

a second set of computer-executable instructions which provides said decrypted data to a software process if said -secure repository trusts said software process (column 3, lines 25-30);

wherein said secure repository establishes trust of said software process at least in part by establishing trust with an intermediate object, said intermediate object comprising a third set of computer-executable instructions dynamically linked to said software process (column 19, lines 45-67).

Examiner supplies the same rationale for the motivation as recited in the rejection of claim 1 to incorporate the teachings of Cassagnol et al within the system Spies et al.

As per claim 21, Spies et al teach software process renders said decrypted data (column 3, line 27).

As per claim 22, Spies et al teach receiving from said intermediate object first data comprising:

second data based at least in part on at least some code contained in said intermediate object (column 17, lines 20-25); and

a signature of said second data; and validating said signature (column 17, lines 25-28).

As per claim 23, Spies et al teach second data comprises a hash of said at least some code (column 18, lines 46-48).

As per claim 24, Spies et al teach fourth set of computer-executable instructions further performs acts comprising:

receiving from said intermediate object second data based at least in part on code contained in said software process (column 17, lines 26-28).

As per claim 25, Spies et al teach issuing a first interface call without regard to whether said one of said plurality of secure repositories is a first of said plurality of secure repositories or a second of said plurality of secure repositories (column 3, line 17);

if said one of said plurality of secure repositories is said first of 8 said plurality of secure repositories, dynamically linking with a first set of computer9 executable instructions invocable by said first interface call (column 17, line 14); and

if said one of said plurality of secure repositories is said second of said plurality of secure repositories, dynamically linking with a second set of computer-executable instructions -invocable by said first interface call, said second said of computer-executable instructions being different from said first set of computer-executable instructions (figure 11, element 174).

Examiner supplies the same rationale for the motivation as recited in the rejection of claim 1 to incorporate the teachings of Cassagnol et al within the system Spies et al.

As per claim 26, Spies et al teach each of said plurality of secure repositories converts encrypted data to decrypted data using a cryptographic algorithm to apply a cryptographic key to said encrypted data (column 3, lines 25-30).

As per claim 27, Spies et al teach first secure repository comprises a software-based secure repository, and wherein said second secure repository comprises at least some isolated hardware (column 17, line 35, column 18, lines 12-13, and column 19, line 9).

As per claim 28, Spies et al teach each of said first and second secure repositories are software-based repositories, said first secure repository having at least one feature not present in said second secure repository (column 17, line 33 and column 18, lines 10-20).

As per claim 30, Spies et al teach a computer-readable medium encoded with a second set of computer-executable instructions to perform the method of claim 25 (column 17, line 33).

As per claim 31, Spies et al teach establishing to said second software process the authenticity of an intermediary object and using said intermediary object to establish to said second software process the authenticity of said first software process (column 17, lines 13-32).

Examiner supplies the same rationale for the motivation as recited in the rejection of claim 1 to incorporate the teachings of Cassagnol et al within the system Spies et al.

As per claim 33, Spies et al teach said operation comprises rendering said decrypted data (column 3, line 27).

As per claim 34, Spies et al teach first software process is a text rendering application, and wherein said decrypted data comprises text (column 17, line 4, column 20, line 46, and column 21, lines 57-60).

As per claim 35, Spies et al teach said intermediary object comprises a set of computer-executable instructions having a first function callable from said first software process, and wherein the act of establishing to said second software process the authenticity of said intermediary object includes, or is actuated by, the act of said first software process calling said first function (column 19, lines 30-61).

As per claim 36, Spies et al teach said act of establishing to said second software process the authenticity of said intermediary object includes the act of providing said second software process with a certificate based at least in part on said set of computer-executable instructions (column 17, lines 13-32).

As per claim 37, Spies et al teach certificate comprises a signed hash of at least some of said computer-executable instructions (column 18, lines 46-49).

As per claim 38, Spies et al teach said intermediary object is in the address space of said first software process, and wherein said first function is referenceable by an address within said address space (column 17, lines 22-23 and figure 10, element 179).

As per claim 39, Spies et al teach said set of computer-executable instructions is dynamically linkable with said first software process, and wherein said method further comprises the act of linking said set of computer-executable instructions with said first software process (column 18, lines 64-67).

As per claim 40, Spies et al teach said intermediary object comprises a set of computer-executable instructions having a first function callable from said first software process, and wherein said act of using said intermediary object to establish to said second software process the authenticity of said first software process includes, or is actuated by, the act of said first software process issuing a call to said first function (column 19, lines 30-61).

As per claim 41, Spies et al teach computer-readable medium encoded with a second set of computer-executable instructions to perform the method of claim 31 (column 17, line 33).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Michael R Vaughan
Examiner
Art Unit 2131

MV

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100